Section II: Administrative Security
Title: Information Security Training and Awareness Standard
Current Effective Date: June 30, 2008
Revision History: June 10, 2008
Original Effective Date: June 30, 2008

Purpose: To define and establish the requirements for the North Carolina (NC) Department of Health and Human Services (DHHS) Information Security Training and Awareness Program.

STANDARD

1.0 Background

All Divisions and Offices management shall ensure that DHHS workforce members are aware of all information security roles and responsibilities. The security standards presented in this document will outline how the Divisions and Offices management, with assistance from the Division Information Security Official (ISO), must create, maintain, and deliver training and awareness to the DHHS workforce members (e.g., business associates, general contractors, third-party contractors, vetted employees, etc.).

2.0 Delivering Security Training and Awareness to DHHS Workforce Members

2.1 Delivering Security Training Programs to DHHS Workforce Members

The Divisions and Offices general information security training must include, but not be limited to the following:

- Acceptable and correct use of information resources
- How to report an information security incident
    - See the NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual – Information Incident Management Policy
- Legal responsibilities associated with information security
    - See the NC DHHS Security Standards, Administrative Security Standards – Information Security and Compliance Management Issues Standard
- Training in information security threats, vulnerabilities, and safeguards
- Annually, general information security training for workforce members (e.g., information security roles and responsibilities)

DHHS workforce members may improve their information security training and awareness knowledge by:

- Obtaining membership in technical clubs, boards, or focus groups
- Receiving subscriptions to technical documents (e.g., newsletters, magazines, and white papers)
- Obtaining self-study and certifications relevant to information security

The Division ISO must notify their Divisions and Offices management of any and all necessary general information security training as it pertains to DHHS workforce members.

2.2 Delivering Security Awareness Programs to DHHS Workforce Members

Division and Office information security awareness communication methods may include, but not be limited to the following:

- Electronic updates such as emails, pamphlets, posters, pop-up messages, newsletters, and other media depending on the complexity of the information security awareness messages.
- Division or Office approved tools that enhance awareness and educate workforce members on information security threats along with appropriate safeguards.
- A workforce member handbook that contains information security awareness policies and standards. It is recommended that the workforce member handbook be formally delivered to and signed by all workforce members within the first sixty (60) days of employment and before workforce members access Divisions and Offices information resources.

2.3 Training Documentation

All Division and Office information security training and awareness documentation must be properly safeguarded. The security training and awareness documentation shall be maintained in accordance with NC Department of Cultural Resources (DCR) – Government Records Branch of NC and the NC Division of Human Resources (HR) – DHHS HR Policy Manual.

2.4 Division ISO and Management General Information Security Training and Awareness Evaluation

Annually, the general information security training and awareness must be reviewed by the Division ISO and the Divisions and Offices management. This will ensure that the general information security awareness training materials are evaluated and updated. The general information security training and awareness for the review must include, but not be limited to the following:

- Introduction of new technologies and associated security risks
- Updates to include new information security risks
- Updates to information security incident response

Participation in the above training and awareness methods must exist only if the participation will provide value to current information security roles and responsibilities.

2.5 Information Security Training and Awareness Feedback

The Division ISO and the appropriate Divisions and Offices management shall receive input from workforce members concerning the effectiveness of current information security training and awareness activities on a periodic basis as determined by Divisions and Offices management. The Division ISO shall ensure that this process is done periodically and that all feedback is recorded and safeguarded accordingly.

References:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 11 – Delivering Training and Staff Awareness, Section 01: Awareness
    - Standard 110101 – Delivering Awareness Programs to Permanent Staff
    - Standard 110102 – Third-Party Contractor: Awareness Programs
    - Standard 110104 – Drafting Top Management Security Communications to Staff
    - Standard 110105 – Providing Regular Information Updates to Staff
  - Chapter 11 – Delivering Training and Staff Awareness, Section 02: Training
    - Standard 110201 – Information Security Training on New Systems
    - Standard 110202 – Information Security Officer: Training
    - Standard 110203 – User: Information Security Training
    - Standard 110204 – Technical Staff: Information Security Training
    - Standard 110205 – Training New Recruits in Information Security

- NC Department of Cultural Resources (DCR)
  - Government Records Branch of NC

- NC Division of Human Resources (HR)
  - DHHS HR Policy Manual

- NC DHHS Security Standards Manual
  - Administrative Security Standards
    - Information Security and Compliance Management Issues Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Security Training and Awareness Policy
  - Information Incident Management Policy